

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-147072

(43)Date of publication of application : 06.06.1997

(51)Int.Cl.

G06K 17/00
A61B 5/117
G06T 7/00
G06K 19/10

(21)Application number : 07-326467

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 21.11.1995

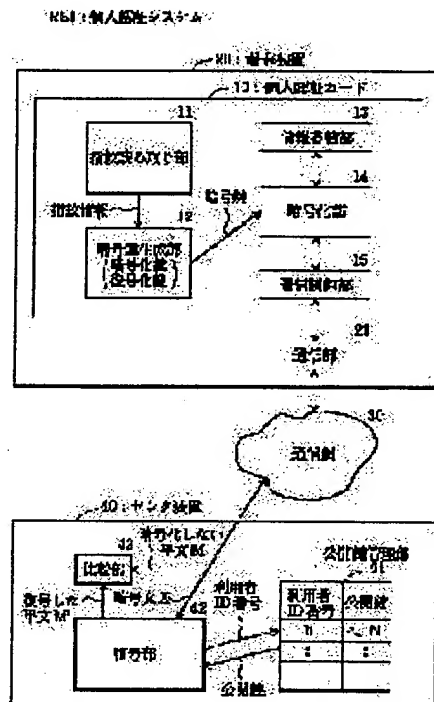
(72)Inventor : TAKANO MASAJI
GOMI KAZUHIRO
MATSUMURA TAKAHIRO
SUGIMURA TOSHIKI

(54) PERSONAL AUTHENTICATION SYSTEM, PERSONAL AUTHENTICATION CARD AND CENTER EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a personal authentication system, personal authentication card and center equipment with which such a trouble that a password number is necessary to be secretly memorized, can be excluded and there is no danger for fingerprint information from being stolen from the card and cables.

SOLUTION: A cryptographic key is generated 12 corresponding to the combination of read fingerprint information and the attribute of personal authentication card, prescribed information is enciphered 14 inside the personal authentication card by the enciphering key of this cryptographic key and the prescribed enciphered information, prescribed non-enciphered information and the ID of user corresponding to the read fingerprint are sent from terminal equipment to center equipment 40. On the other hand, the received prescribed enciphered information is deciphered 42 while using an open key corresponding to the ID of user received from terminal equipment 20, this prescribed deciphered information is compared with the received prescribed non-enciphered information and when both the information are equal to each other, it is judged that user is given personal authentication.



LEGAL STATUS

[Date of request for examination]

14.10.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

特開平9-147072

(43) 公開日 平成9年(1997)6月6日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 17/00			G 0 6 K 17/00	V
				S
A 6 1 B 5/117		0277-2J	A 6 1 B 5/10	3 2 2
G 0 6 T 7/00			G 0 6 F 15/62	4 6 0
G 0 6 K 19/10			G 0 6 K 19/00	S
審査請求 未請求 請求項の数 7 F D (全 6 頁)				

(21) 出願番号 特願平7-326467

(22) 出願日 平成7年(1995)11月21日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 高野 正次

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(72) 発明者 五味 和洋

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(72) 発明者 松村 隆宏

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74) 代理人 弁理士 川久保 新一

最終頁に続く

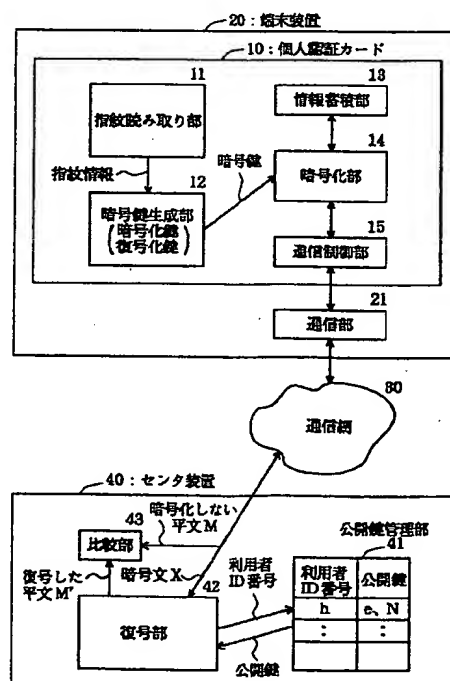
(54) 【発明の名称】 個人認証システム、個人認証カードおよびセンタ装置

(57) 【要約】

【課題】 暗証番号を秘密に記憶しておくという煩雑性を排除でき、また、指紋情報がカード、ケーブルから盗まれる心配がない個人認証システム、個人認証カードおよびセンタ装置を提供することを目的とするものである。

【解決手段】 読み取った指紋情報と個人認証カードの属性との組み合わせに応じて暗号鍵を生成し、この暗号鍵のうちの暗号化鍵によって、個人認証カード内で所定情報を暗号化し、暗号化された所定情報と暗号化されていない所定情報と読み取られた指紋に対応する利用者のIDとを端末装置がセンタ装置に送出し、一方、端末装置から受信した利用者のIDに対応した公開鍵を使用して、受信した暗号化所定情報を復号し、この復号された所定情報と受信した暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断するものである。

RS1: 個人認証システム



【特許請求の範囲】

【請求項1】 指紋を読み取る指紋読み取り手段と；上記指紋の読取情報と個人認証カードの属性との組み合わせに応じた暗号鍵を生成する暗号鍵生成手段と；上記生成された暗号鍵のうちの暗号化鍵によって所定情報を暗号化する暗号化手段と；を個人認証カードが有し、上記暗号化された所定情報と、暗号化されていない上記所定情報と、上記読み取られた指紋に対応する利用者のIDとを送出する信号送出手段を端末装置が有し、各利用者に対応して公開鍵を記憶する公開鍵管理手段と；上記通信網から送信された上記利用者のIDに対応して上記公開鍵管理手段から読み出された上記公開鍵を使用することによって、上記通信網を介して送信された上記暗号化された所定情報を復号する復号手段と；この復号手段によって復号された所定情報と、上記通信網を介して送信された上記暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断する比較手段と；をセンタ装置が有することを特徴とする個人認証システム。

【請求項2】 請求項1において、上記個人認証カードの属性は、上記個人認証カード毎に異なるものであることを特徴とする個人認証システム。

【請求項3】 請求項1において、上記暗号鍵生成手段は、上記指紋の読取情報を所定の関数によって指紋特徴量に変換する指紋特徴量変換手段と；複数の素数を格納し、上記指紋特徴量変換手段が出力した指紋特徴量に応じた素数を、上記複数の素数から出力する素数格納手段と；を有するものであることを特徴とする個人認証システム。

【請求項4】 請求項1において、上記個人認証カードは、上記指紋を読み取った時刻を上記センタ装置に送出し、上記センタ装置は、上記個人認証カードから送出された上記時刻と、上記比較手段が比較すべき時刻との差が所定の時間差を越えている場合には、個人認証されたと判断しないものであることを特徴とする個人認証システム。

【請求項5】 指紋を読み取る指紋読み取り手段と；上記指紋の読取情報と個人認証カードの属性との組み合わせに応じた暗号鍵を生成する暗号鍵生成手段と；上記生成された暗号鍵のうちの暗号化鍵によって所定情報を暗号化する暗号化手段と；上記個人認証カードの利用者のIDと、上記暗号化された所定情報と、暗号化されない所定情報とを送出する通信制御部と；を有することを特徴とする個人認証カード。

【請求項6】 請求項5において、上記個人認証カードを開くと、上記個人認証カードの属性が消失するものであることを特徴とする個人認証カード。

【請求項7】 各利用者に対応して公開鍵を記憶する公

開鍵管理手段と；暗号化された所定情報を復号化する復号化手段と；通信網から送信された利用者のIDに対応し、上記公開鍵管理手段から読み出された上記公開鍵を使用することによって、通信網を介して送信された暗号化された所定情報を復号する復号手段と；この復号手段によって復号された所定情報と、上記通信網を介して送信された暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断する比較手段と；を有することを特徴とするセンタ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、銀行のキャッシュサービス等のように、通信を利用した高度かつ重要なサービスを利用する際に、サービスセンタ等のセンタ装置への不正なアクセスを防止し、利用者個人の正当性を確認する認証技術に関するものである。

【0002】

【従来の技術】 銀行のキャッシュサービス等において、磁気カードやICカード等によって個人を認証する場合、第1の従来方法では、そのカードが所有者本人に使用されていることを証明するために、利用者に暗証番号を入力させている。この場合、カードの所有者は、予め決められた暗証番号を記憶しておく必要があり、カードの所有者が暗証番号を記憶していなければならないという煩雑性がある。

【0003】

【発明が解決しようとする課題】 つまり、第1の従来方法では、正規の所有者のみが記憶しているパスワードのような秘密情報によって個人認証を行うので、個人認証カードの所有者に暗証番号を秘密に記憶させる必要があるという問題がある。

【0004】 この煩雑性を回避する方法として、暗証番号を使用する代わりに指紋を使用して、個人を認証する第2の従来方法が提案されている。

【0005】 この第2の従来例では、スキャナのような指紋を読み取る手段と、認証すべき利用者個人の指紋を予め記憶する手段と、読み取った指紋と記憶している指紋との一致を判断する手段とが設けられている。

【0006】 しかし、これらの手段が、センタ装置とは独立して設けられているので、各カードに記憶されている指紋情報が盗まれる危険性があるという問題がある。また、カードを使用する端末装置とセンタ装置との間で、ケーブル等を介して、上記指紋情報を交信する必要があり、上記指紋情報に関する秘密情報が、そのケーブルを介して、外部に漏洩する危険性があるという問題がある。

【0007】 本発明は、暗証番号を秘密に記憶しておくという煩雑性を排除でき、また、指紋情報がカード、ケーブルから盗まれる心配がない個人認証システム、個人認証カードおよびセンタ装置を提供することを目的とす

るものである。

【0008】

【課題を解決するための手段】本発明は、指紋を読み取る指紋読み取り手段と、指紋の読取情報と個人認証カードの属性との組み合わせに応じた暗号鍵を生成する暗号鍵生成手段と、生成された暗号鍵のうちの暗号化鍵によって所定情報を暗号化する暗号化手段とを個人認証カードに設け、暗号化された所定情報と、暗号化されていない上記所定情報と、読み取られた指紋に対応する利用者のIDとを端末装置が送出し、各利用者に対応して公開鍵を記憶する公開鍵管理手段と、通信網から送信された利用者のIDに対応して公開鍵管理手段から読み出された公開鍵を使用することによって、送信された暗号化された所定情報を復号する復号化手段と、この復号手段によって復号された所定情報と、上記通信網を介して送信された暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断する比較手段とをセンタ装置に設けたものである。

【0009】

【発明の実施の形態および実施例】図1は、本発明の一実施例である個人認証システムRS1を示すブロック図である。

【0010】個人認証システムRS1は、個人認証カード10と、端末装置20と、通信網30と、センタ装置40とを有するものである。

【0011】個人認証カード10は、指紋読み取り部11と、暗号鍵生成部12と、情報蓄積部13と、暗号化部14と、通信制御部15とを有する。

【0012】指紋読み取り部11は、利用者の指が押し当てられたときに、圧力等を微細に検出し、指紋の画像情報（指紋情報）を読み取るものである。

【0013】暗号鍵生成部12は、個人認証カード10の属性を有し、指紋読み取り部11が読み取った指紋情報と個人認証カード10の属性との組み合わせに応じた暗号鍵を生成するものである。なお、上記「暗号鍵」は、「暗号化鍵」と「復号化鍵」とを含むものである。また、上記実施例において、個人認証カード10の属性は、図2に示すように、指紋特徴量変換部50と素数表Tとによって抽出される素数である。

【0014】情報蓄積部13は、通信文Mとしての所定情報（通信文Mには利用者のID番号が含まれる）を蓄積するものである。

【0015】暗号化部14は、暗号鍵生成部12によって生成された暗号鍵のうちの暗号化鍵によって所定情報を暗号化するものである。

【0016】通信制御部15は、個人認証カード10の利用者のIDと、上記暗号化された所定情報と、暗号化されない所定情報とを送出する通信制御部である。

【0017】端末装置20は、通信網30を介してセンタ装置40と交信する通信部21を有する。通信部21

は、暗号化された所定情報と、暗号化されていない所定情報と、読み取られた指紋に対応する利用者のIDとをセンタ装置40に送出するものである。なお、図1には、端末装置20として通信部21のみが記載されているが、他の機能をも有し、これらを省略して図示してある。

【0018】センタ装置40は、公開鍵管理部41と、復号部42と、比較部43とを有する。

【0019】公開鍵管理部41は、各利用者に対応して公開鍵を記憶する手段である。復号部42は、通信網30から送信された利用者のIDに対応して公開鍵管理部41から読み出された公開鍵を使用することによって、暗号化部14で暗号化され、通信網30を介して送信された所定情報を復号する手段である。段と；比較部43は、復号部42によって復号された所定情報と、通信網30を介して送信され、暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断する比較手段である。

【0020】図2は、個人認証システムRS1における暗号鍵生成部12を説明する図である。

【0021】暗号鍵生成部12は、指紋の読取情報を関数Fによって指紋特徴量に変換する指紋特徴量変換部50と、複数の素数 p 、 q 、 u 、 v 、 w 、……を、上記指紋特徴量に対応して格納し、上記指紋特徴量変換手段が出力した指紋特徴量に応じた2つの素数 p 、 q を、上記複数の素数から出力する素数表（素数格納手段）とを有するものである。

【0022】なお、上記実施例において、暗号化の方式として、公開鍵暗号方式の1つであるRSA暗号方式を用いている。

【0023】次に、上記実施例における個人認証動作について説明する。

【0024】まず、利用者は、個人認証カード10上の指紋読み取り部11に指を押し当て、指紋情報を読み込ませる。この読み取られた指紋情報は暗号鍵生成部12に送られ、指紋情報は関数Fによって指紋特徴量に変換され、この変換された指紋特徴量に応じて、素数表Tから2つの素数 p 、 q が出力される。なお、素数表Tには、たとえば51桁の素数が焼き付けられ、素数表Tに格納されている素数またはその配列は、個人認証カード10毎に異なっている。また、関数Fは、指紋読み取り部11に指が当てられたときに、その当て方や圧力によって、関数値が変動しない頑強さを持つように作られている。

【0025】上記の場合、利用者毎に指紋情報が異なり、また、暗号鍵生成部12における素数表Tの内容が個人識別カード10毎に異なるので、暗号鍵生成部12が出力する2つの素数 p 、 q は、結果的に、利用者と個人識別カード10との組み合わせに応じてユニークに定まる。換言すれば、別の利用者が上記個人認証カード1

0を利用すると、別の素数の組み(たとえば、 r と s)が選択される。

【0026】そして、暗号鍵生成部12から出力された素数 p と q とは、暗号化部14に送られる。暗号化部14において、素数 p と q とに応じて、RSA暗号方式に必要な公開鍵 e 、 N と、復号化鍵 d とを、以下のようにして生成する。

【0027】まず、

N : 素数 p と q の積、

L : $p-1$ と $q-1$ の最小公倍数、

e : L と素な数、

d : L 、 e に対して $1 = Le + ed$ を満足する数である。

【0028】つまり、 $(p-1)$ と $(q-1)$ との最小公倍数 L を求め、この最小公倍数 L と素な数として公開鍵 e を求め、また、 $p \times q = N$ によって残りの公開鍵 N を求める。また、 $1 = Le + ed$ を満足する復号化鍵 d を求める。この手順については、たとえば、「太田、黒澤、渡辺: 情報セキュリティの科学、95年、講談社、pp. 133」に開示されている。

【0029】なお、公開鍵 e 、 N は、利用者ID番号に対応して、公開鍵管理部41に保管されている。

【0030】ところで、情報蓄積部13には、センタ装置40との間でやりとりされる通信文 M が蓄積されている。この通信文 M は、センタ装置40との間で予め定められたフォーマットで蓄積され、たとえば、個人認証カード10の製造番号(ID番号)、利用者の個人ID番号、カードリーダの製造番号(ID番号)、利用開始時刻等の情報が、上記通信文 M に含まれる。

【0031】暗号化部14では、暗号鍵生成部12から暗号化鍵を受け取り、発信する通信文 M (平文)を暗号文 X に変換する。この場合、

$$X = M^e \pmod{N}$$

の式を使用する。ここで、 x^y は、 x の y 乗であり、 $z \pmod{w}$ は、 z を w で割った余りであり、 d は、復号化鍵である。

【0032】また、通信制御部15は、端末装置20の通信部21を用いて、最適なプロトコルによって、暗号文 X と、通信文 M (暗号文 X に対応する平文、利用者IDを含む)とをセンタ装置40に対して送信する。

【0033】次に、センタ装置40における利用者の認証動作について説明する。

【0034】まず、復号部42は、受信した通信文 M の中から、利用者ID、具体的には利用者ID番号 h を抽出し、この抽出された利用者ID番号 h に対応して公開鍵管理部41に保管されている公開鍵 e と N とを公開鍵管理部41から読み出す。そして、 $M' = X^e \pmod{N}$ の式に従って、センタ装置40が受信した暗号文 X を平文 M' に復号する。

【0035】このようにして復号された平文 M' と暗号

化せずに受信した通信文 M とが一致するか否かを比較部43が調べ、復号された平文 M' と暗号化せずに受信した通信文 M とが一致すれば、その暗号文 X の発信者が正規の利用者であることを、センタ装置40が認証する。

【0036】ここで、第三者が、センタ装置40から公開鍵 e と N と不正に盗み、さらに、個人認証させようとしたとする。しかし、RSA暗号方式では、公開鍵 e と N とに基づいて、素数 p 、 q を導くことは、実効的には不可能であり、現在の計算機能力では、公開鍵 e と N とに基づいて素数 p 、 q を導くには、数百年以上かかるといわれている。上記実施例においては、素数 p 、 q 、 d 等の素数の情報がなければ、平文 M から暗号文 X を導くことはできないので、個人認証に必要な暗号文 X を作ることができず、したがって、センタ装置40における復号部42で復号化する対象としての暗号文 X を復号部42に送り込むことができず、不正に個人認証を行わせることができない。

【0037】また、上記実施例において、端末装置20からセンタ装置40に送られる通信文 M の中には、個人認証カード10によって個人認証を開始する時刻、つまり利用開始時刻の情報が含まれており、センタ装置40において、その利用開始時刻と実際の時刻との差を演算し、この差の時間が所定時間を経過していれば、個人認証しないようにしてある。すなわち、正規の利用者が個人認証カード10を使用して個人認証している間に、第三者が不正に、暗号鍵、通信文 M 等を盗用したとしても、その後、その第三者が個人認証させようとした場合、その時刻が遅くなるので、個人認証がされず、安全性が高い。

【0038】さらに、上記実施例において、不正な第三者が、個人認証カード10を不正に入手し、正規の利用者になりすまして通信を開始しようとしたときには、指紋読み取り部11が出力する指紋情報は、正規の利用者による指紋情報と異なるので、関数 F によって選ばれる素数の組みが p 、 q 以外のものになり、このような素数によって暗号化した暗号をセンタ装置40においては復号できないので、誤って個人認証されることがない。

【0039】ところで、上記実施例において、利用者の指紋情報そのものは、個人認証カード10から外に出ず、また、個人認証カード10内のどこにも記憶蓄積されないで、正規の利用者の指紋情報が第三者に盗まれることはない。また、利用者の指紋情報そのものをセンタ装置40にも記憶していないので、この点からも、正規の利用者の指紋情報が第三者に盗まれることはない。

【0040】さらに、個人認証カード10自体を入手し、この個人認証カード10のケースを開けて内部情報を見ることによって、素数 p と q や関数 F や素数表 T の中身を見破られる場合が考えられるが、この対策として、以下のようなことが考えられる。

① 素数表 T の内容を直接カードの外へは読み出せない

10

20

30

40

50

機構を個人認証カード10に付加する。

② 個人認証カード10が開けられた場合には、個人認証カード10内に記憶されている情報が全て消失する構成を採用する。

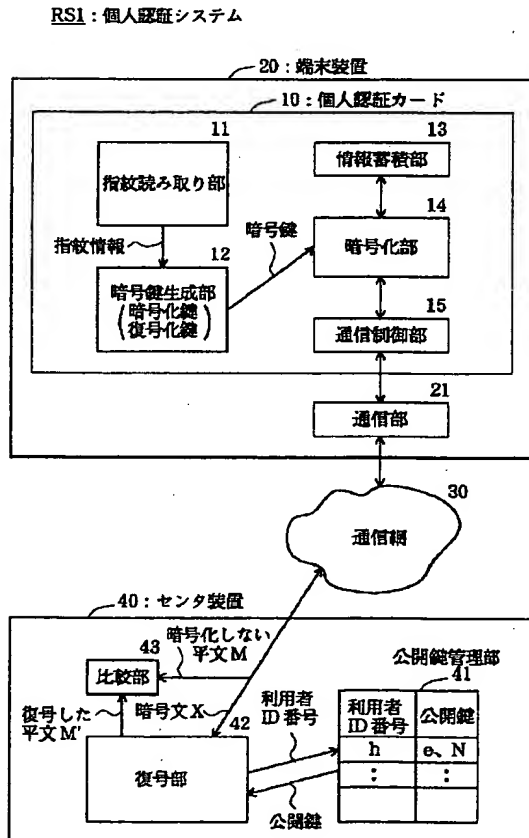
③ 素数表T上の素数のエントリ数を多くすることによって、正しい素数の組みpとqが発見される確率を低くし、これによって、正しい素数の組みpとqが発見されることを実効的に困難にする。

【0041】また、上記実施例において、暗号鍵生成部12が出力する情報は、指紋情報と個人認証カード10によって割り当てられた適当な素数であり、これは暗号化のための情報に過ぎない。したがって、素数がたとえ盗聴され解読されたとしても、指紋情報そのものは不正な第三者に盗まれることがない。上記実施例においては、実際には、センタ装置40の保守者や個人認証カード10の所有者自身も、自分の指紋情報そのものを知り得ない。

【0042】なお、上記実施例において、暗号鍵生成部12における素数表Tの内容が、どの個人識別カード10においても同じであるようにしても、上記と同様の動作を行う。

【0043】

【図1】



【発明の効果】本発明によれば、個人の認証に必要な秘密情報である指紋情報そのものは、個人認証カードの外部には出ず、また、個人認証カード内のどこにも記憶蓄積されないので、重大な問題となりうる個人の指紋情報そのものが漏洩される危険性がないという効果を奏する。

【図面の簡単な説明】

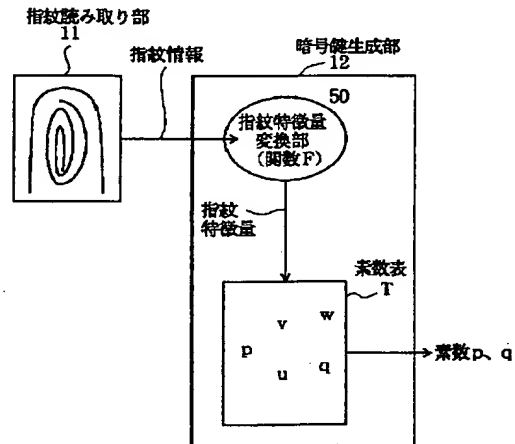
【図1】本発明の一実施例である個人認証システムRS1を示すブロック図である。

【図2】個人認証システムRS1における暗号鍵生成部12を説明する図である。

【符号の説明】

10…個人認証カード、
11…指紋読み取り部、
12…暗号鍵生成部、
13…情報蓄積部、
14…暗号化部、
20…端末装置、
40…センタ装置、
50…指紋特徴量変換部、
T…素数表。

【図2】



フロントページの続き

(72)発明者 杉村 利明

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内